SECTION 9—INFORMATION WARFARE TECHNOLOGY

OVERVIEW

Information warfare (IW) is defined as actions taken to achieve information superiority by affecting adversary information, information based processes, information systems and computer based networks while defending one's own information, information based processes, information systems, and computer based networks. IW is a combination of both old roles and missions evolving and adapting to a new environment and new revolutionary capabilities. IW includes both offensive and defensive activities: electronic warfare (EW), physical destruction, deception, information attack, psychological operations, operational security, IW protection and security measures. IW depends upon and embodies related information systems and other supporting technologies. Computer hacking is a form of IW just as is bombing an adversary's C^2 facility since both deny the enemy information. Because of the dependency of military C^4I^2 systems on both civil and military communications, the crossover between civil and military communications is transparent. This section focuses on the technology areas shown in the box above that contain militarily critical technologies. No militarily critical technologies were identified in two other technology areas: Deception and Psychological Operations. For related technologies see Section 5 - Electronics, 8 - Information Systems, 15 - Sensors and Lasers, 16 - Signature Control and 17 - Space Systems.

[1] Also called Electronic Countermeasures (ECM).

[2] Also called Electronic Counter-Countermeasures (ECCM).

SECTION 9.1—ELECTRONIC ATTACK

OVERVIEW

An early historical example of Electronic Attack (EA)[1] is the Allies' jamming of the giant German Wurzburg radar. The radio frequency (RF) jamming confused the radar's gating mechanism, making few aircraft appear as many. These measures were also used against anti-aircraft radar with considerable success. The increase in the capability of electronic countermeasures grew with the increased use of radio frequency (RF) devices for guidance and control of weapons systems and the concurrent advances in electronics. Add to this capability the sophisticated countering modulations that can be stored as a library of computer algorithms, and the operations of electronic warfare (EW) take on unusual depth. Thus, since the end of World War II, many complex and intricate techniques have been devised to counter the newest weapons systems.

Table 9.1-1. Electronic Attack Militarily Critical Technology Parameters

TECHNOLOGY	Militarily Critical Parameters Minimum Level to Assure US Superiority	Critical Materials	Unique Test, Production, and Inspection Equipment	Unique Software and Parameters	Control Regimes
ECM ANTENNA	< –40 dBm	None identified	Compact range	None identified	WA ML 11
AID & DIA: AUTO RECOGNITION	> 12 bps and 10 GHz	ROM DSP	None identified	None identified	WA ML 11
SYNTHESIZERS	> – 60 dBm, 2–18 GHz	DSP	None identified	None identified	WA ML 11 WA IL Cat 3
RF: WIDEBAND ADAPTIVE POLARIZERS	Null depth > 25 dB Bandwidth > 20%	None identified	None identified	None identified	WA ML 11
DIGITAL RF MEMORIES	Digital memories with clock rate > 200 MHz;	SS power devices	None identified	None identified	WA IL Cat 3
SOLID STATE AMPLIFIERS	2–18 GHz, 10 watt, 40%	None identified	Public domain	None identified	WA IL Cat 4
ECM SIMULATION	Simulations incorporating validated algorithms involving one or more operational or developmental military systems.	None identified	Built-ins	In encryption module	WA ML 11
ESM: RECEIVER DIGITIZATION	10 Gbits samples < 15 W @ 8 bits	None identified	Instrumented antenna range	None identified	WA ML 11
ESM: ANTENNA ARRAYS	< 0.1° DOA accuracy	None identified	Max bandwidth oscilloscope built-in	None identified	WA ML 11
ESM: RF DELAY LINES	> 2 GHz; < 6 dB NFg; > 500 n sec delay	HTS materials	Max bandwidth oscilloscope	None identified	WA ML 11
ESM: SWITCHED DELAY LINES	0.4 dB filter with low sensitivity loss; 20 MHz bandwidth @ 40 dB; 10 µsec switching	HTS materials	Max bandwidth oscilloscope	Steering algorithms	WA ML 11
ESM: LOW RCS ANTENNA	Effective area out of band < effective area in band	HTS materials	Hi tech range (laboratory)	Steering algorithms	WA ML 11
HIGH TEMP SUPERCONDUCTING ANTENNA (ESM)	Size: < 1/4 wavelength	None identified	Hi tech range (laboratory)	Acquisition algorithms	WA ML 11
ESM: MINIATURE MMW INTEGRATED RECEIVER	< 5 dB NF; 75 GHz bandwidth	Detector sensitivity	Isolation, sensitivity and sel test	Ranging formula	WA ML 11
PRECISION PASSIVE RANGING	CEP < 0.1% of range	None identified	None identified	None identified	None

[1] Also called Electronic Countermeasures (ECM).

SECTION 9.2—ELECTRONIC PROTECTION

OVERVIEW

Electronic Protection (EP)[2] are those measures used to defeat electronic attack (EA). The EP device must detect the countermeasure, such as jamming or electronic deception, and use active decoys, RF traps and synchronizers, and devices that read through spectral noise. The vast majority of these "fixes" are derived by the developers and manufacturers of the electronic weapon systems as self protective measures.

Table 9.2-1. Electronic Protection Militarily Critical Technology Parameters

TECHNOLOGY	Militarily Critical Parameters Minimum Level to Assure US Superiority	Critical Materials	Unique Test, Production, and Inspection Equipment	Unique Software and Parameters	Control Regimes
DIGITAL RF MEMORIES	Digital memories with clock rate > 200 MHz	None identified	None identified	Compact codes	WA IL Cat 11
SIGNAL SYNTHESIS SOFTWARE	Accuracy > 98%	None identified	None identified	Mimic accuracy	WA ML 11
SEE-THROUGH FILTERING	Comb Filters; Narrow sloped filters < 0.5°	None identified	None identified	Filter codes	WA ML 11

[2] Also called Electronic Counter-Countermeasures (ECCM).

SECTION 9.3—OPTICAL COUNTERMEASURES

OVERVIEW

In past MCTL compilations, optical countermeasures were listed under the general field of electronic attack (EA). The increased use of optical devices in many weapon systems necessitated a separate field for this important technology. Optical countermeasures (OCM) include lasers, remote sensing television, the plethora of IR devices, UV sensors, spectrometers, radiometers, and hyperspectral and multispectral devices plus a number of decoys. The OCM field will continue to grow and require more sophisticated answers in the future.

Table 9.3-1. Optical Countermeasures Militarily Critical Technology Parameters

TECHNOLOGY	Militarily Critical Parameters Minimum Level to Assure US Superiority	Critical Materials	Unique Test, Production, and Inspection Equipment	Unique Software and Parameters	Control Regimes
SEMICONDUCTOR LASER: INCL COHERENT AND NON-COHERENT SOURCES	3–12 microns; 200 milliwatts avg power; 1 watt peak power per pulse; 100 µsec pulse width; 75° K operating temperature	None identified	Molecular beam expitaxy production equipment	IR jamming techniques. DIRCM pointing/tracking algorithms	WA IL Cat 6 WA ML 11
SOLD STATE LASERS: INCL COHERENT AND SS SOURCES	3 lines in 1.5–5.0 µ band > 20 kHz PRF	OPOs, CW Pump Diodes > 50 °C, Dichroric coatings	OPO production processes	IR jamming techniques	WA ML 11 WA IL Cat 6
NON-COHERENT ARC LAMPS	Braze temperature > 1400 °C	Proprietary metalizing and brazing materials	High temperature vacuum ovens	IR jamming techniques	WA ML 11
IR DETECTORS AND ARRAYS	EW technical parameters are less stringent than IRST or F4R and imaging missile requirements	InSe, HgCdTe, PtSi, Cryo Coolers	Array production techniques	OCM/OCCM Rx	WA ML 11
UV DETECTOR AND MICROCHANNEL PLATES	Photon thruput efficiency > 50 °C operating temperatures	UV filters	Filter production; microchannel plate production	Critical Element: Temporal; and Spatial	WA ML 11 WA IL Cat 3
CLOSED LOOP IR COUNTERMEASURE	6:1 S/N ratio; > – 105 dBm sensitivity	Detectors, optics, trackers, FFT processors	Algorithms and software test eq.	FFT: analyzers	WA ML 11
VISUALLY COVERT CHEMICAL SOURCES	1200 w/sr, 3–5 µ per condela	Pyrophonic solids spectrally sources	Radiometric squid	None identified	None
SPATIALLY TAILORED EXPENDABLE SOURCES; AIRBORNE	1:3 side to rear 1:5 front to rear	Shielded sources	Radiometric squid	None identified	None
SELF IGNITING PYROTECHNIC SOURCES	Rise time < 0.2 sec to peak	Pyrophonic metal igniters	Radiometric squid	None identified	None
AIR LAUNCH KINETIC DECOYS	Operate up to Mach 1.0 at sea level	Propelled aerodynamic decoys	Radiometric squid	None identified	None

SECTION 9.4—OPTICAL COUNTER-COUNTERMEASURES

OVERVIEW

Optical Counter-Countermeasures (OCCM) are measures taken to counter optical countermeasures (OCM). As with electronic protection (EP), this means building into optically pointed weapons systems devices that can detect and counter or defeat the OCM. Multispectral, multiband, and adaptive frequency devices are common but can sometimes be defeated by wideband, high-power devices.

Table 9.4-1. Optical Counter-Countermeasures Militarily Critical Technology Parameters

TECHNOLOGY	Militarily Critical Parameters Minimum Level to Assure US Superiority	Critical Materials	Unique Test, Production, and Inspection Equipment	Unique Software and Parameters	Control Regimes
SIGNAL SYNTHESIS SOFTWARE	Accuracy > 98%	None identified	None identified	None identified	WA ML 11
SPECTRALLY MOLDED IR SOURCES	Temperature > 1000° C airborne and Temperature > 350 K shipborne when viewed in 2–3 and 3–5 µ bands	Pyroten liquids Pyrophoric solids	None identified	None identified	WA ML 11
SYNTHESIZERS	FOV 0.5 deg Two-color seeker > 1 KHz bandwidth > 270 deg blanking	None identified	None identified	Computer target matching	WA ML 11